

dvcsvr

102 $\sim \beta \leftarrow h(\pi)$
 104 $\sim \rho \leftarrow_R \{0, 1\}^\lambda$
 106 $\sim \gamma \leftarrow E_{pk_{svr}}(\langle \beta, \rho \rangle)$
 108 $\sim \delta \leftarrow \text{mac}_a(\langle \gamma, \tau \rangle)$

γ, δ, τ
 110 \rightarrow

$\langle a, b, c \rangle \leftarrow D_{sk_{svr}}(\tau) \sim 112$
 abort if $\text{mac}_a(\langle \gamma, \tau \rangle) \neq \delta \sim 114$
 $\langle \beta, \rho \rangle \leftarrow D_{sk_{svr}}(\gamma) \sim 116$
 abort if $(\beta \neq b) \sim 118$
 $\eta \leftarrow \rho \oplus c \sim 120$

η
 $\leftarrow 122$

124 $\sim sk \leftarrow \rho \oplus \eta \oplus f(v, \pi)$
 126 \sim abort if $M(pk_{dvc}, sk) \neq 1$
 128 \sim return sk

FIG. 1

dvcsvr

202 ~ $\beta \leftarrow h(\pi)$
 204 ~ $\rho \leftarrow_R \{0,1\}^\lambda$
 206 ~ $r \leftarrow_R \{0,1\}^{\kappa_{sig}}$
 208 ~ $\gamma \leftarrow E_{pk_{svr}}(\langle m, r, \beta, \rho \rangle)$
 210 ~ $\delta \leftarrow \text{mac}_a(\langle \gamma, \tau \rangle)$

γ, δ, τ
 212 \rightarrow

$\langle a, b, u, d_2, N \rangle \leftarrow D_{sk_{svr}}(\tau)$ ~ 214
 abort if $\text{mac}_a(\langle \gamma, \tau \rangle) \neq \delta$ ~ 216
 $\langle m, r, \beta, \rho \rangle \leftarrow D_{sk_{svr}}(\gamma)$ ~ 218
 abort if $\beta \neq b$ ~ 220
 $v \leftarrow (\text{encode}(m, r))^{d_2} \bmod N$ ~ 222
 $\eta \leftarrow \rho \oplus v$ ~ 224

η
 226 \leftarrow

228 ~ $v \leftarrow \rho \oplus \eta$
 230 ~ $d_1 \leftarrow f(v, \pi)$
 232 ~ $s \leftarrow v(\text{encode}(m, r))^{d_1} \bmod N$
 234 ~ abort if $s^e \not\equiv_N \text{encode}(m, r)$
 236 ~ return $\langle s, r \rangle$

FIG. 2

dvcsvr

300

302 ~ abort if $\text{valid}(c) = 0$
 304 ~ $\beta \leftarrow h(\pi)$
 306 ~ $\rho \leftarrow_R \{0, 1\}^{\lambda+2|q|}$
 308 ~ $\gamma \leftarrow E_{pk_{svr}}(\langle c, \beta, \rho \rangle)$
 310 ~ $\delta \leftarrow \text{mac}_a(\langle \gamma, \tau \rangle)$

 γ, δ, τ

312

$\langle a, b, u, p, q, g, x_2 \rangle \leftarrow D_{sk_{svr}}(\tau) \sim 314$
 abort if $\text{mac}_a(\gamma, \tau) \neq \delta \sim 316$
 $\langle c, \beta, \rho \rangle \leftarrow D_{sk_{svr}}(\gamma) \sim 318$
 abort if $\beta \neq b \vee \text{valid}(c) = 0 \sim 320$
 $w \leftarrow \text{select}(c) \sim 322$
 $v \leftarrow w^{x_2} \bmod p \sim 324$
 $r \leftarrow_R \mathbb{Z}_q \sim 326$
 $v' \leftarrow w^r \bmod p \sim 328$
 $e \leftarrow h_{zkp}(\langle v, v', g^r \bmod p \rangle) \sim 330$
 $s \leftarrow x_2 e + r \bmod q \sim 332$
 $\eta \leftarrow \rho \oplus \langle v, e, s \rangle \sim 334$

 η

336

338 ~ $\langle v, e, s \rangle \leftarrow \rho \oplus \eta$
 340 ~ $w \leftarrow \text{select}(c)$
 342 ~ abort if $e \neq h_{zkp}(\langle v, w^s v^{-e} \bmod p, g^s(y_2)^{-e} \bmod p \rangle)$
 344 ~ $x_1 \leftarrow f(v, \pi)$
 346 ~ $\mu \leftarrow w^{x_1} \bmod p$
 348 ~ return $\text{reveal}(v\mu \bmod p, c)$

FIG. 3

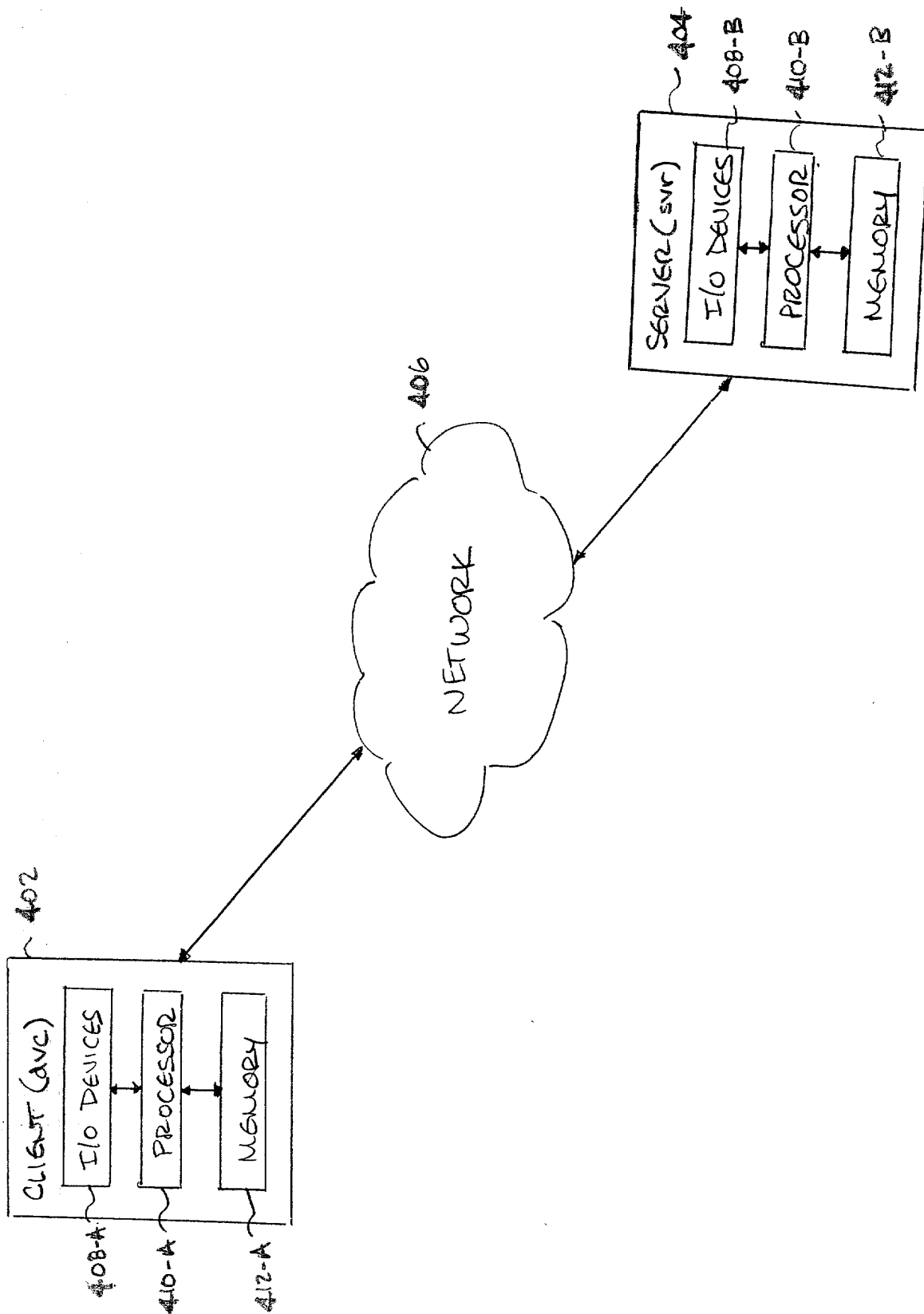


FIG. 4